

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-148049

(43)Date of publication of application : 29.05.2001

(51)Int.Cl.

G07F 7/12
 G06F 17/60
 G06F 19/00
 G06K 17/00
 G06K 19/10
 G07F 7/08
 G07F 7/10

(21)Application number : 11-329083

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 19.11.1999

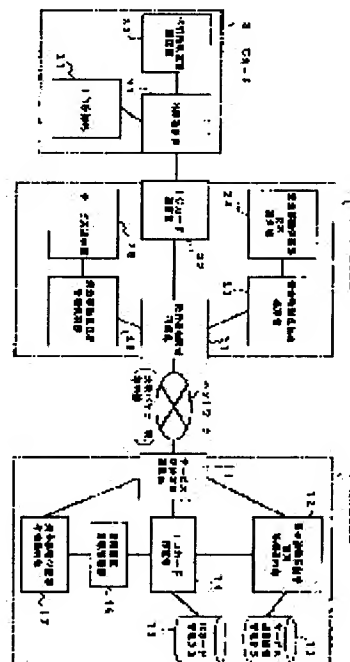
(72)Inventor : MORITA TETSUYUKI
 MUTO NOBUO
 HORI MASAHIRO
 OKUYAMA HIRONOBU

(54) PROXY COLLECTION SYSTEM AND METHOD, AND RECORDING MEDIUM WITH PROXY COLLECTION PROGRAM RECORDED THEREON

(57)Abstract:

PROBLEM TO BE SOLVED: To make local currency value creation by a malicious person meaningless and also to make safely performable transactions between a plurality of service providing devices existing at many places and a settlement acting center.

SOLUTION: A proxy collection device 1 manages currency value information while making the currency value information correspond to the identification information(ID) of an IC card, and the card 3 holds only the ID proper to the card made to correspond to the currency value information managed by the representative settlement device and does not have the currency value information locally. When the card 3 is inputted, the service providing device 2 performs proxy collection to the device 1, and transmits a fund transfer certificate request demanding the sending of a fund transfer certificate, and the device 1 prepares a fund transfer certificate ensuring that a proxy-collected amount is deposited to a designated deposit destination and transmits the fund transfer certificate to the device 2.



* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1]A system by which a vicarious execution collection device carries out vicarious execution collection of the service money amount which a service provision system and a vicarious execution collection device of card use are mutually connected by a network, transmits and receives a transfer-of-fund guarantee demand and a transfer-of-fund guarantee, and a service provision system serves, comprising:

A means by which a vicarious execution collection device receives a transfer-of-fund guarantee demand from a service provision system.

A means which carries out mutual recognition to a card.

A means to relate with identification information of a card and to manage money value information.

Provide a means to draw up a transfer-of-fund guarantee which guarantees supplying the amount of money for vicarious execution collection to a specific partner, and to transmit to a service provision system, and a service provision system, A means to create a transfer-of-fund guarantee demand which performs vicarious execution collection and requires dispatch of a transfer-of-fund guarantee, and to transmit to a vicarious execution collection device, A means to hold identification information of the card concerned related with money value information which possesses a means to receive and manage a transfer-of-fund guarantee from a vicarious execution collection device, and a means to provide service for a card user, and in which a vicarious execution collection device manages a card, and a means which carries out mutual recognition to a vicarious execution collection device.

[Claim 2]A system by which a vicarious execution collection device carries out vicarious execution collection of the service money amount which a service provision system and a vicarious execution collection device of card use are mutually connected by a network, transmits and receives a transfer-of-fund guarantee demand and a transfer-of-fund guarantee, and a service provision system serves, comprising:

A means by which a vicarious execution collection device receives a transfer-of-fund guarantee demand from a service provision system.

A means which carries out mutual recognition to a card.

A means to relate with identification information of a card, and a delivery destination of the amount of money for vicarious execution collection, and to manage money value information.

Provide a means to draw up a transfer-of-fund guarantee which guarantees having supplied the amount of money for vicarious execution collection to a specific partner, and to transmit to a service provision system, and a service provision system, A means to create a transfer-of-fund guarantee demand which performs vicarious execution collection and requires dispatch of a transfer-of-fund guarantee, and to transmit to a vicarious execution collection device, A means to hold identification information of the card concerned related with money value information which possesses a means to receive and manage a transfer-of-fund guarantee from a vicarious execution collection device, and a means to provide service for a card user, and in which a vicarious execution collection device manages a card, and a means which carries out mutual recognition to a vicarious execution collection device.

[Claim 3] A service provision system and a vicarious execution collection device of card use are a vicarious execution collecting method in a system mutually connected by a network, and a service provision system, When vicarious execution collection use is received from a card user, create a transfer-of-fund guarantee demand which performs vicarious execution collection and requires dispatch of a transfer-of-fund guarantee, transmit to a vicarious execution collection device and a vicarious execution collection device, If a transfer-of-fund guarantee demand is received, a card and mutual recognition are performed and mutual recognition is successful, Incorporate identification information stored in a card and the amount of money for vicarious execution collection indicated to a transfer-of-fund guarantee demand is reduced from money value information related with said identification information, Draw up a transfer-of-fund guarantee which guarantees delivery of the amount of money for vicarious execution collection to an amount-of-money delivery destination for vicarious execution collection indicated to a transfer-of-fund guarantee demand, transmit to a service provision system and a service provision system, A vicarious execution collecting method characterized by what a transfer-of-fund guarantee from a vicarious execution collection device is received and managed, and is served for a card user.

[Claim 4] A service provision system and a vicarious execution collection device of card use are a vicarious execution collecting method in a system mutually connected by a network, and a service provision system, When vicarious execution collection use is received from a card user, create a transfer-of-fund guarantee demand which performs vicarious execution collection and requires dispatch of a transfer-of-fund guarantee, transmit to a vicarious execution collection device and a vicarious execution collection device, If a transfer-of-fund guarantee demand is received, a card and mutual recognition are performed and mutual recognition is successful, Incorporate identification information stored in a card and the amount of money for vicarious execution collection indicated to a transfer-of-fund guarantee demand is reduced from money value information related with said identification information, It increases to money value information related with an amount-of-money delivery destination for vicarious execution collection indicated to a transfer-of-fund guarantee demand, Draw up a transfer-of-fund guarantee which guarantees that the amount of money for vicarious execution collection ends with delivery to an amount-of-money delivery destination for vicarious execution collection indicated to a transfer-of-fund guarantee demand, transmit to a service provision system and a service provision system, A vicarious execution collecting method characterized by what a transfer-of-fund guarantee from a vicarious execution collection device is received and managed, and is served for a card user.

[Claim 5] In the vicarious execution collecting method according to claim 3 or 4, a vicarious execution collection device, A vicarious execution collecting method characterized by what a service provision system inspects an electronic signature of a transfer-of-fund guarantee, it saves this transfer-of-fund guarantee if it is a right signature, and an electronic signature of the vicarious execution collection device concerned is added to a transfer-of-fund guarantee, and it transmits to a service provision system, and it serves.

[Claim 6] In the vicarious execution collecting method according to claim 3, 4, or 5, a service provision system, A vicarious execution collecting method characterized by what an electronic signature of the service provision system concerned will be added to a transfer-of-fund guarantee demand, and it will transmit to a vicarious execution collection device, a vicarious execution collection device inspects an electronic signature of a transfer-of-fund guarantee demand, this transfer-of-fund guarantee demand will be saved, and a card and mutual recognition will be performed for if it is a right signature.

[Claim 7] A recording medium storing a vicarious execution collection program for performing processing of the vicarious execution collecting method according to claim 3, 4, 5, or 6 by computer and in which computer reading is possible.

[Translation done.]

*** NOTICES ***

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the recording medium which recorded a vicarious execution collection system using an IC card etc., a method for the same, and a vicarious execution collection program.

[0002]

[Description of the Prior Art]The vicarious execution collection system which generally used the card, The system (following, former) of the kind which has monetary value in a card like common bus cards by the place which manages monetary value, A center manages monetary value, and a user is giving identification information, such as ID (ID:Identifier), to a center, and is classified into two with the systems (following, latter) of the kind which operates the monetary value in a center and performs vicarious execution collection. Itself can become money and monetary value here is data of electronic money.

[0003]The former is a system which enables settlement of accounts on a local, when money value information is electronically recorded into the card which the user who requests vicarious execution collection owns and a service provision system reads the money value information. As this system, prepaid type vicarious execution collection systems which are circulating widely now, such as U card and KUOKADO, are mentioned besides common bus cards. However, in the vicarious execution collection system which has money value information in the card which exists locally, creation of electronic values is local and may be performed. A vicarious execution collection contractor in the system which performs vicarious execution collection so that it may be represented by the pachinko card. It became the system that not a user individual but the contractor who requests vicarious execution collection from a vicarious execution collection system got cash according to forged electronic values easily, and there was a risk of an organization-based crime being performed at the place which is not connected in a network, i.e., the place which directly a vicarious execution collection contractor does not show.

[0004]The latter is a vicarious execution collection system with which a vicarious execution collection center manages all the money value information of the user who requests vicarious execution collection in a unified manner at one place. When a user has ID by which correlation with the money value information which a settlement-of-accounts vicarious execution center manages was made and a user notifies the information on the vicarious execution collection request which contains ID in a settlement center, a vicarious execution collection center changes the money value information in a vicarious execution collection center, and supplies settlement amount to the requested point. Therefore, money value information does not come out of a center, and monetary value creation on a local has the advantage of not being made.

[0005]Conventionally, there is AKOSHISU used, for example on the Internet in this center mold system. In AKOSHISU, it reports that a vicarious execution collection center communicates with a vendor's host at every request of the vicarious execution collection from a user, and performs vicarious execution collection to it, and a vendor's host will give his service to a user, if this notice is received. Management of the dealings with a vicarious execution collection center and dealings is easy, since this host was in one place, after collection vicarious execution, money was certainly

paid to the vendor, establishment of the confidential relation between a settlement agent and a vendor was possible by the means of the notice of mere transaction data, and the vendor was easy establishment.

[0006]However, when two or more service provision systems like a vending machine divide and exist in multi spot, management of the dealings with a vendor and a vicarious execution collection contractor and dealings is difficult. Therefore, the injustice of the malicious vendor or the malicious settlement-of-accounts acting agent was also considered, and the reliable dealings with a vendor and a vicarious execution collection contractor were difficult in the means of the notice of the conventional mere transaction data. Although the method with which a vendor's host does central control of the trade managing is also considered by conducting dealings with a vicarious execution collection center and two or more service provision systems through one host of a vendor as a trade managing means, there is a problem that this requires communication cost.

[0007]

[Problem(s) to be Solved by the Invention]In the vicarious execution collection system using a card, while improper or the purpose of this invention shall be meaningless, creation of the monetary value in the local by those malicious, It is in being able to carry out by feeling easy about dealings with two or more service provision systems and settlement-of-accounts vicarious execution centers, and holding down communication cost. [multi spot]

[0008]

[Means for Solving the Problem]In order for this invention to make it possible for a vicarious execution collection device which performs vicarious execution collection to conduct unjust dealings which are not with two or more service provision systems [multi spot], A service provision system transmits a transfer-of-fund guarantee demand to a vicarious execution collection device, and draw up a transfer-of-fund guarantee exchanged for monetary value between delivery destinations of specification of the amount of money in which a vicarious execution collection device carried out vicarious execution collection, and it transmits to a service provision system, A service provision system is characterized [biggest] by saving this transfer-of-fund guarantee. a Prior art is considering it as a center management type system which does not have money value information locally, and a vicarious execution collection system using a transfer-of-fund guarantee, and enabling unjust dealings with a service provision system in multi spot which are not and about which he can feel easy differ.

[0009]It is constituted from a vicarious execution collection system of this invention by IC card etc. which can store identification information (ID:Identifier) related with a vicarious execution collection device which manages a vicarious execution collection user's money value information, two or more service provision systems, and money value information of a vicarious execution collection device. In this invention, an IC card owner has already owned an IC card related with money value information, and an IC card owner assumes that money value information in a vicarious execution collection device is paid.

[0010]A vicarious execution collection device is provided with an IC card authentication means, a money-value-information management tool, a transfer-of-fund guarantee preparing means, an electronic signature means, etc. A delivery destination name of a transfer-of-fund guarantee identifier, the amount of money for vicarious execution collection, and the amount of money for vicarious execution collection, etc. are described by transfer-of-fund guarantee, and a vicarious execution collection subject's electronic signature is further added to it. It is defined as this transfer-of-fund guarantee being what guarantees passing the amount of money to a delivery destination of the amount of money in which a vicarious execution collection device carried out vicarious execution collection in exchange for a transfer-of-fund guarantee demand. A transfer-of-fund guarantee identifier is considering it as the only thing (for example, consecutive numbers) in all the transfer-of-fund guarantees, and it is effective in guaranteeing the only nature of a transfer-of-fund guarantee. By making it a name which the amount of money for vicarious execution collection is effective in specifying the amount of money which carries out vicarious execution collection, sees socially a delivery destination name of the amount of money for vicarious execution collection, and is matched with an only thing, The delivery point of the amount of money for vicarious execution collection is specified, a meaning which reproduces a transfer-of-

fund guarantee by the 3rd person by this is abolished, and it is effective in preventing injustice.

[0011]A service provision system is provided with a transfer-of-fund guarantee request means, a transfer-of-fund guarantee management preserving means, a service provision means, etc. It is defined as a transfer-of-fund guarantee demand being a command required as transmitting a transfer-of-fund guarantee in which a delivery destination of the amount of money for vicarious execution collection and the amount of money for vicarious execution collection was described to a service provision system. The amount of money for vicarious execution collection is effective in specifying the amount of money by which vicarious execution collection is carried out, and a delivery destination of the amount of money for vicarious execution collection is effective in a vicarious execution collection device specifying a partner who exchanges monetary value for a transfer-of-fund guarantee.

[0012]An IC card is provided with an authentication means of ID holding mechanism and a vicarious execution collection device, etc., and is constituted. ID is the identification information (Identifier) related with money value information of a vicarious execution collection device. With an IC card, a user of composition of that mutual recognition can be carried out with a vicarious execution collection device, and ID cannot be altered except a vicarious execution collection device defines it as what is carried and made. If it is a thing of same composition in this invention, generally arbitrary cards are available.

[0013]A vicarious execution collection user has the IC card related with money value information of a vicarious execution collection device. If a user with an IC card inputs an IC card into a service provision system and tells vicarious execution collection use volition, a service provision system will create a transfer-of-fund guarantee demand, and will transmit to a vicarious execution collection device. If a transfer-of-fund guarantee demand is received from a service provision system, a vicarious execution collection device will perform first an IC card and mutual recognition which were inputted into a service provision system, and will read ID in an IC card. Next, a vicarious execution collection device looks for money value information relevant to read ID, and reduces the amount of money demanded by transfer-of-fund guarantee demand. Next, a vicarious execution collection device draws up a transfer-of-fund guarantee, adds an electronic signature to a transfer-of-fund guarantee using information which only a vicarious execution collection device can know, and transmits this transfer-of-fund guarantee to a service provision system. If a transfer-of-fund guarantee is received, the contents of the transfer-of-fund guarantee and a signature investigate whether it is a right thing, and if a service provision system is right, it saves a transfer-of-fund guarantee. Then, a service provision system gives its service to a vicarious execution collection user. A saved transfer-of-fund guarantee is passed to a delivery destination of the amount of money for vicarious execution collection written in a transfer-of-fund guarantee in a certain form, and a delivery destination of the amount of money for vicarious execution collection exchanges a transfer-of-fund guarantee for monetary value represented by cash between vicarious execution collection devices.

[0014]According to this vicarious execution collection system, he feels easy without a vicarious execution collection device and a prior contract, and the service provision system can use vicarious execution collection. This is because each service provision system receives directly a transfer-of-fund guarantee which is monetary value from a vicarious execution collection device.

[0015]In another mode of this invention, a vicarious execution collection device has the money value information of a delivery destination of the amount of money for vicarious execution collection, reduces it from money value information related with an IC card in the amount of money for vicarious execution collection in response to a transfer-of-fund guarantee demand from a service provision system, and is moved to money value information of a delivery destination of the amount of money for vicarious execution collection. In this case, it is defined as a transfer-of-fund guarantee being a bond showing a vicarious execution collection device having moved the amount of money for vicarious execution collection to money value information of a delivery destination of the amount of money which carried out vicarious execution collection from money value information corresponding to an IC card. A transfer-of-fund guarantee saved at a service provision system has an effect which protects from a vicarious execution collection device injustice of a vicarious execution collection device where the amount of money for vicarious execution collection

is not supplied to money value information of a delivery destination of the amount of money for vicarious execution collection.

[0016]According to this mode, there is no necessity of treating monetary value outside a vicarious execution collection device, and there is an effect whose creation of worth of a local becomes impossible.

[0017]In another mode of this invention, a service provision system has a means to sign a transfer-of-fund guarantee demand using information which only a service provision system can know, and a signature using information which only a service provision system can know is attached to a transfer-of-fund guarantee demand. A vicarious execution collection device inspects a signature of a transfer-of-fund guarantee demand, if it is a right signature, will save this transfer-of-fund guarantee demand, and will start mutual recognition with an IC card.

[0018]

[Embodiment of the Invention]Hereafter, the 1 embodiment of this invention is described in detail using a drawing.

[0019][Example 1] Drawing 1 shows the example of whole construction of the vicarious execution collection system with which this example 1 is applied. In drawing 1, the vicarious execution collection device with which 1 performs vicarious execution collection, the service provision system with which two or more 2 exists in multi spot, and 3 are IC cards which a user owns.

[0020]the vicarious execution collection device 1 -- the service provision system 2 and a network (a digital data exchange packet.) (A modem etc. being represented as for this) with the service provision system communications department 11 which communicates via a dedicated line etc., and the transfer-of-fund guarantee request administrator preserving part 12 which manages and saves a transfer-of-fund guarantee demand, The service provision system management data base (service provision system management DB) 13 holding the public key of each service provision system 2, etc., IC card 3, the IC card authentication section 14 which performs mutual recognition, and the IC card database (IC card DB) 15 holding the common key corresponding to each IC card for performing IC card 3 and mutual recognition, etc., It comprises the money-value-information Management Department 16 which manages the money value information related with the ID number stored in IC card 3, and the transfer-of-fund guarantee creation preserving part 17 which draws up a transfer-of-fund guarantee and adds the signature of the vicarious execution collection device 1 concerned.

[0021]An example of the money value information which the money-value-information Management Department 16 of the vicarious execution collection device 1 manages is shown in drawing 2. In drawing 2, it is shown that the amount of a cash deposit which is the money value information corresponding to the ID number "00001" stored in the IC card is 20000 yen. The same may be said of an ID number "00002" and "00003." Each IC card owner pays in the predetermined amount of money beforehand.

[0022]The vicarious execution collection device communications department 21 which the service provision system 2 gives communication with the vicarious execution collection device 1, IC card 3 and the IC card communications department 22 represented with the IC card read/write (R/W) which communicates, The transfer-of-fund guarantee demand part 23 which receives the volition of vicarious execution collection use from an IC card owner, and creates a transfer-of-fund guarantee demand, It comprises the transfer-of-fund guarantee demand signature part 24 which adds the signature of the service provision system concerned to a transfer-of-fund guarantee demand, the transfer-of-fund guarantee management preserving part 25 which records and saves the transfer-of-fund guarantee sent from the vicarious execution collection device 1, and the service provision section 26 which actually gives its service to a vicarious execution collection user.

[0023]IC card 3 comprises the external communication part 31 and the vicarious execution collection device 1 which communicate with the service provision system 2, the vicarious execution collection device authentication section 32 which performs mutual recognition, and the ID attaching part 33 holding the ID number related with the money value information of the vicarious execution collection device 1.

[0024]In the vicarious execution collection device 1, the service provision system communications

department 11 relays communication with the transfer-of-fund guarantee request administrator preserving part 12, the IC card authentication section 14 and the transfer-of-fund guarantee creation preserving part 17, and the service provision system 2 through a network. The transfer-of-fund guarantee request administrator preserving part 12 communicates with service provision system management DB13 and the IC card authentication section 14. The IC card authentication section 14 communicates with IC card management DB15 and the money-value-information Management Department 16 further. The money-value-information Management Department 16 communicates with the transfer-of-fund guarantee creation preserving part 17 further.

[0025]In the service provision system 2, the vicarious execution collection device communications department 21 relays communication with the transfer-of-fund guarantee demand part 23 and the transfer-of-fund guarantee management preserving part 25, and the vicarious execution collection device 1 through a network. The IC card communications department 22 communicates with IC card 3, and if necessary, it will relay communication with the vicarious execution collection device 1 and IC card 3 via the vicarious execution collection device communications department 21. The transfer-of-fund guarantee demand part 23 communicates with the transfer-of-fund guarantee demand signature part 24 further. The transfer-of-fund guarantee management preserving part 25 communicates with the service provision section 26 further.

[0026]In IC card 3, the external communication part 31 relays communication with the vicarious execution collection device authentication section 32 and the ID attaching part 33, and the vicarious execution collection device 1 through the service provision system 2.

[0027]Next, operation of this example is explained. A user inputs IC card 3 into the service provision system 2, and performs volition of vicarious execution collection use. As for the service provision system 2, if the transfer-of-fund guarantee demand part 23 receives the volition of vicarious execution collection use from an IC card owner via the IC card communications department 22 and the vicarious execution collection device communications department 21, the transfer-of-fund guarantee demand part 23 will create a transfer-of-fund guarantee demand. The delivery destination name of a service provision system name, the amount of money of vicarious execution collection, and the amount of money for vicarious execution collection, a transfer-of-fund guarantee demand number, the date and time of creation of a transfer-of-fund guarantee demand, the network address of the service provision system 2 concerned, etc. are described by transfer-of-fund guarantee demand. A service provision system name is effective in specifying the device which requires vicarious execution collection, and the amount of money for vicarious execution collection is effective in specifying the amount of money by which vicarious execution collection is carried out. The delivery destination of the amount of money for vicarious execution collection is effective in the vicarious execution collection device 1 specifying cash and the point to pass in exchange for a transfer-of-fund guarantee, and it is effective in abolishing the meaning which uses by stealth the 3rd person's transfer-of-fund guarantee, and preventing the theft of a transfer-of-fund guarantee. A transfer-of-fund guarantee demand number is an identifier used only once by a service provision system, and there are this transfer-of-fund guarantee demand number and an effect of specifying a transfer-of-fund guarantee demand as an only thing by the date and time of creation. The network address of a service provision system has an effect which notifies the place on the network of the service provision system 2.

[0028]Next, the transfer-of-fund guarantee demand part 23 transmits, and the transfer-of-fund guarantee demand created to the transfer-of-fund guarantee demand signature part 24 the transfer-of-fund guarantee demand signature part 24, An electronic signature is added using the secret key which only the service provision system 2 concerned can know to a transfer-of-fund guarantee demand, and if it changes with an alteration and ***** is prevented, it will return to the transfer-of-fund guarantee demand part 23. Specifying the service provision system which created the transfer-of-fund guarantee demand by this electronic signature, It analyzes the service provision system with which the IC card was used, and it is not only useful for information gathering of holding an IC card user's use trend, but when injustice should be performed, there is an effect used as one information for unjust pursuit.

[0029]The service provision system 2 transmits the transfer-of-fund guarantee demand with a signature returned to the transfer-of-fund guarantee demand part 23 to the vicarious execution

collection device 1 via the vicarious execution collection device communications department 21. An example of the transfer-of-fund guarantee demand transmitted to the vicarious execution collection device 1 is shown in drawing 3.

[0030]The service provision system communications department 11 receives the transfer-of-fund guarantee demand with a signature from the service provision system 2, and the vicarious execution collection device 1 sends it to the transfer-of-fund guarantee request administrator preserving part 12. If it judges that the transfer-of-fund guarantee request administrator preserving part 12 inspects the electronic signature of a transfer-of-fund guarantee demand using the public key of the service provision system 2 currently held to service provision system management DB13, and is a right signature, The contents which saved this transfer-of-fund guarantee demand, and were described by the transfer-of-fund guarantee demand at the IC card authentication section 14 are notified. The saved transfer-of-fund guarantee demand is effective in the service provision system 2 serving as proof of surely having requested vicarious execution collection to the vicarious execution collection device 1 concerned.

[0031]Next, the IC card authentication section 14 is held IC card management DB15. The network address of the service provision system 2 described by the transfer-of-fund guarantee demand using a common key to origin. The vicarious execution collection device authentication section 32 and mutual recognition of IC card 3 are performed via the service provision system communications department 11, the vicarious execution collection device communications department 21 of the service provision system 2 and the IC card communications department 22, and the external communication part 31 of IC card 3. Mutual recognition is processing which checks that two persons have the confidential information which only a partner or the limited person can know mutually, and judges who a partner is mutually. For example, the challenge response method using a common key is common. If mutual recognition is successful, IC card 3 will report that the flag which enables the vicarious execution collection device authentication section 32 to read an ID number to the ID attaching part 33 is built, and the IC card authentication section 14 will read an ID number from the IC card attaching part 33 of this IC card 3. Then, the IC card authentication section 14 sends the contents described by the ID number and transfer-of-fund guarantee demand which were read to the money-value-information Management Department 16. The money-value-information Management Department 16 reduces the amount of money for vicarious execution collection indicated to the transfer-of-fund guarantee demand from the money value information related with the ID number, and sends the contents described by the transfer-of-fund guarantee demand to the transfer-of-fund guarantee creation preserving part 17.

[0032]The transfer-of-fund guarantee creation preserving part 17 draws up a transfer-of-fund guarantee, adds an electronic signature using the secret key which only this vicarious execution collection device 1 can know, and transmits to the service provision system 2 via the service provision system communications department 11. The transfer-of-fund guarantee creation preserving part 17 saves this transfer-of-fund guarantee. As for a transfer-of-fund guarantee, the delivery destination name of a transfer-of-fund guarantee number, a corresponding transfer-of-fund guarantee demand number, the amount of money for vicarious execution collection, and the amount of money for vicarious execution collection, etc. are described. A transfer-of-fund guarantee is monetary value which guarantees passing the amount of money to the delivery destination of the amount of money in which the vicarious execution collection device 1 carried out vicarious execution collection in exchange for this transfer-of-fund guarantee, A transfer-of-fund guarantee number has an effect which shows the only nature of the published transfer-of-fund guarantee, A transfer-of-fund guarantee demand number is effective in taking correspondence with the transfer-of-fund guarantee to publish, the amount of money for vicarious execution collection is effective in specifying the amount of money which carries out vicarious execution collection, and the delivery destination name of the amount of money for vicarious execution collection is effective in specifying the point which can receive the amount of money by which vicarious execution collection was carried out.

[0033]While the vicarious execution collection device 1 saves at drawing 4, an example of the transfer-of-fund guarantee transmitted to the service provision system 2 is shown. This shows the transfer-of-fund guarantee published corresponding to the transfer-of-fund guarantee demand of

drawing 3.

[0034]The vicarious execution collection device communications department 21 receives the transfer-of-fund guarantee with an electronic signature sent from the vicarious execution collection device 1, and the service provision system 2 sends it to the transfer-of-fund guarantee management preserving part 25. If the electronic signature added to the transfer-of-fund guarantee investigates whether it is what surely was made by the vicarious execution collection device 1 and confirms that it is a just transfer-of-fund guarantee, the transfer-of-fund guarantee management preserving part 25, This transfer-of-fund guarantee is saved, it reports that its service is given to the service provision section 26, and the service provision section 26 gives its service to an IC card owner. The saved transfer-of-fund guarantee will be passed to the delivery destination of the amount of money for vicarious execution collection written in this transfer-of-fund guarantee, and the delivery destination of the amount of money for vicarious execution collection will exchange cash for a transfer-of-fund guarantee between the vicarious execution collection devices 1.

[0035]According to the system of drawing 1, what is necessary is just to hold ID related with the money value information which the vicarious execution collection device 1 manages to IC card 3, and it is not necessary to have money value information in it. As this effect, even if the Tampa-proof structure of an IC card is broken, it becomes impossible to increase value creation, i.e., the amount of money, only on a local etc. Since the delivery destination of the amount of money for vicarious execution collection and the amount of money are being fixed, even if the 3rd person performs injustice, the structure where this 3rd person gets profits does not become, but the transfer-of-fund guarantee saved at the service provision system 2 can prevent the 3rd person's injustice. Since the sex is guaranteed to the transfer-of-fund guarantee by the transfer-of-fund guarantee number uniquely [the], it is impossible for the delivery destination of the amount of money for vicarious execution collection to also reproduce a transfer-of-fund guarantee, and to obtain profits. A transfer-of-fund guarantee guarantees thoroughly passing the amount of money for vicarious execution collection to the delivery destination of the amount of money for vicarious execution collection in exchange for this transfer-of-fund guarantee, and can also prevent the injustice of the vicarious execution collection device 1, and the dealings and trade managing of the service provision system 2 and the vicarious execution collection device 1 of it about which he can feel easy become possible.

[0036]An example of the processing sequence of this example is shown in drawing 5. The owner of IC card 3 already pays cash to the vicarious execution collection device 1, and this is a basis of the situation where the vicarious execution collection device 1 is ending with increase about the amount of cash received to the money value information corresponding to this IC card 3, The processing sequence of Example 1 until the service provision system 2 which received the use volition of vicarious execution collection communicates with the vicarious execution collection device 1, requests vicarious execution collection and gives its service by an IC card owner by receiving a transfer-of-fund guarantee from the vicarious execution collection device 1 is shown. Here, the vending machine of juice is used as the service provision system 2 by using a vicarious execution collection center as the vicarious execution collection device 1, and sale of can juice is made into an example as service.

[0037]An IC card owner inserts IC card 3 in the vending machine 2, pushes the button of desired can juice, and notifies the use volition of vicarious execution collection to the vending machine 2 (S11). The vending machine 2 creates the transfer-of-fund guarantee demand required as performing vicarious execution collection to the vicarious execution collection center 1 (S12). The delivery destination name of a vending machine name, the amount of money of vicarious execution collection, and the amount of money for vicarious execution collection, a transfer-of-fund guarantee demand number, the date and time of creation of a transfer-of-fund guarantee demand, the network address of the vending machine 2, etc. are described by transfer-of-fund guarantee demand. A vending machine name specifies the device which requires vicarious execution collection, and the amount of money for vicarious execution collection specifies the amount of money of the can juice by which vicarious execution collection is carried out. Since the vicarious execution collection center 1 specifies cash and the point to pass in exchange for a transfer-of-

fund guarantee, the delivery destination of the amount of money for vicarious execution collection abolishes the meaning which uses by stealth the 3rd person's transfer-of-fund guarantee, and can prevent the theft of a transfer-of-fund guarantee. A transfer-of-fund guarantee demand number and the date and time of creation can specify a transfer-of-fund guarantee demand as an only thing by making a transfer-of-fund guarantee demand number into the identifier only once used with a vending machine. The network address of a vending machine notifies the place on the network of the vending machine 2. The vending machine 2 adds an electronic signature with the secret key which only the vending machine 2 concerned can know to a transfer-of-fund guarantee demand (S13), and transmits this transfer-of-fund guarantee demand with a signature to the vicarious execution collection center 1 (S14).

[0038]The vicarious execution collection center 1 saves this transfer-of-fund guarantee demand, if the electronic signature of the received transfer-of-fund guarantee demand is a thing of the vending machine 2 to be sure and it checks that the transfer-of-fund guarantee demand is not altered (A11) (A12). The saved transfer-of-fund guarantee demand serves as proof that surely the vending machine 2 requested vicarious execution collection from the vicarious execution collection center 1, at the time of an ex post facto trouble, etc. Next, the vicarious execution collection center 1 performs IC card 3 and mutual recognition (A13, I11). The challenge response method etc. which used the common key perform mutual recognition, and the method which cannot be decoded or cannot be copied performs it with vending machines 2 other than IC card 3 and authentication device 1. If mutual recognition is successful, reading of ID stored in this IC card of IC card 3 will be made possible, the vicarious execution collection center 1 will require reading of ID from IC card 3 (A14), and IC card 3 will notify ID to the vicarious execution collection center 1 (I12).

[0039]The vicarious execution collection center 1 reduces the amount of money indicated to the transfer-of-fund guarantee demand from the money value information corresponding to ID received from IC card 3 (A15). Next, the vicarious execution collection center 1 draws up a transfer-of-fund guarantee (A16). The delivery destination name etc. of the transfer-of-fund guarantee demand number to which the vicarious execution collection center 1 is the monetary value which guarantees passing the above-mentioned amount of money to the delivery destination of the amount of money for vicarious execution collection in exchange for a transfer-of-fund guarantee, and a transfer-of-fund guarantee corresponds with a transfer-of-fund guarantee number, the amount of money for vicarious execution collection, and the amount of money for vicarious execution collection are described. A transfer-of-fund guarantee number shows the only nature of the published transfer-of-fund guarantee, and a transfer-of-fund guarantee demand number takes correspondence with the transfer-of-fund guarantee to publish. The amount of money for vicarious execution collection specifies the amount of money which carries out vicarious execution collection, and the delivery destination name of the amount of money for vicarious execution collection specifies the point which can receive the amount of money by which vicarious execution collection was carried out. Next, after it adds an electronic signature to a transfer-of-fund guarantee using the secret key which only the vicarious execution collection center 1 concerned can know, and the vicarious execution collection center 1 alters, it changes and prevents ***** (A17), it transmits this transfer-of-fund guarantee with a signature to the vending machine 2 (A18).

[0040]If a transfer-of-fund guarantee is received from the vicarious execution collection center 1, the vending machine 2, Check the electronic signature of this transfer-of-fund guarantee (S15), and it is investigated whether the contents written in the transfer-of-fund guarantee agree with the contents demanded by the transfer-of-fund guarantee demand (S16). If normal, this transfer-of-fund guarantee is saved (S17), and can juice is provided to an IC card owner (S18). Then, the saved transfer-of-fund guarantee will be passed to the delivery destination of the amount of money for vicarious execution collection written in this transfer-of-fund guarantee, and the delivery destination of the amount of money for vicarious execution collection will exchange cash for a transfer-of-fund guarantee between the vicarious execution collection centers 1.

[0041]According to the processing sequence of drawing 5, the communication with the vending machine 2 and the vicarious execution collection center 1, If the time of communication with IC card 3 is removed, when transmitting a transfer-of-fund guarantee demand to the vicarious

execution collection center 1 from the vending machine 2, The center which is restricted to 2 times with the time of transmitting a transfer-of-fund guarantee to the vending machine 2 from the vicarious execution collection center 1, for example, carries out central control of the vending machine is installed independently, it lets this center pass, and the case where dealings with a vending machine and a vicarious execution collection center are conducted shows that time communication is reduced clearly.

[0042][Example 2] A vicarious execution collection device has the money value information of the delivery destination of the amount of money for vicarious execution collection, and this example moves the amount of money for vicarious execution collection from the money value information related with the IC card to the money value information of the delivery destination of the amount of money for vicarious execution collection in response to a service provision system to a transfer-of-fund guarantee demand. In this example, the meaning which a transfer-of-fund guarantee has differs from the case of previous Example 1. That is, in Example 1, in order that a transfer-of-fund guarantee might be passed to the delivery destination of the amount of money for vicarious execution collection and the delivery destination of this amount of money for vicarious execution collection might exchange cash for a transfer-of-fund guarantee between vicarious execution collection devices, the transfer-of-fund guarantee had monetary value. On the other hand, since movement of money value information is completed within a vicarious execution collection device in the case of this example, although a transfer-of-fund guarantee does not have monetary value, it has a meaning as a bond (**** finishing bond) used as proof that monetary value moved.

[0043]Since it is fundamentally the same, the overall system configuration of this example is abbreviated to drawing 1. However, in addition to the money value information related with the ID number stored in IC card 3, the money-value-information Management Department 16 in the vicarious execution collection device 1 manages the money value information related with the delivery destination of the amount of money for vicarious execution collection. An example of the money value information which the money-value-information Management Department 16 manages in this example is shown in drawing 6. Here, "ABC incorporated company, "DEF, Inc.", "Japanese Taro", etc. show the delivery destination name of the amount of money for vicarious execution collection. However, ID is able to become delivery destination, above-mentioned company name, and personal name's delivery origin.

[0044]Next, the system configuration of drawing 1 explains operation of this example 2. A user inputs IC card 3 into the service provision system 2, and performs volition of vicarious execution collection use. In the service provision system 2, the transfer-of-fund guarantee demand part 23 receives the volition of the vicarious execution collection use from a system IC card owner, and a transfer-of-fund guarantee demand is created. The delivery destination name of a service provision system name, the amount of money of vicarious execution collection, and the amount of money for vicarious execution collection, a transfer-of-fund guarantee demand number, the date and time of creation of a transfer-of-fund guarantee demand, the network address of the service provision system 2 concerned, etc. are described by transfer-of-fund guarantee demand. In the case of this example, a transfer-of-fund guarantee demand has a meaning requested so that the service provision system 2 supplies the amount of money for vicarious execution collection to the money value information related with the applicable delivery destination from the money value information related with IC card 3 to the vicarious execution collection device 1. That is, the delivery destination of the amount of money for vicarious execution collection in a transfer-of-fund guarantee demand has a meaning which specifies the money value information of the point which the vicarious execution collection device 1 supplies the amount of money for vicarious execution collection in response to this transfer-of-fund guarantee demand. The meaning which other descriptive contents in a transfer-of-fund guarantee demand have is fundamentally [as the case of previous Example 1] the same. The transfer-of-fund guarantee demand part 23 sends the created transfer-of-fund guarantee demand to the transfer-of-fund guarantee demand signature part 24, and the transfer-of-fund guarantee demand signature part 24 adds an electronic signature using the secret key which only the service provision system 2 concerned can know to a transfer-of-fund guarantee demand, and it returns it to the transfer-of-fund guarantee demand part 23.

[0045]The service provision system 2 transmits the transfer-of-fund guarantee demand with a signature of the service provision system 2 concerned returned to the transfer-of-fund guarantee demand part 23 to the vicarious execution collection device 1 via the vicarious execution collection device communications department 21. An example of the transfer-of-fund guarantee demand transmitted to the vicarious execution collection device 1 is shown in drawing 7. This is fundamentally [as the contents of drawing 3] the same.

[0046]The vicarious execution collection device 1 sends the transfer-of-fund guarantee with a signature from the service provision system 2 to the transfer-of-fund guarantee request administrator preserving part 12 through the service provision system communications department 11. If it judges that the transfer-of-fund guarantee request administrator preserving part 12 inspects the electronic signature of a transfer-of-fund guarantee demand using the public key of the service provision system 2 currently held to service provision system management DB13, and is a right signature, The contents which saved this transfer-of-fund guarantee demand, and were described by the transfer-of-fund guarantee demand at the IC card authentication section 14 are notified. The saved transfer-of-fund guarantee demand serves as proof that surely the service provision system 2 requested vicarious execution collection to the vicarious execution collection device 1.

[0047]The IC card authentication section 14 is a challenge response method etc. using the common key currently held at the IC card Management Department 15, Based on the network address of the service provision system 2 described by the transfer-of-fund guarantee demand, the vicarious execution collection device authentication section 32 and mutual recognition of IC card 3 are performed via the service provision system communications department 11-vicarious execution collection device communications department 21-IC card communications department 22-external communication part 31. If mutual recognition is successful, it will report that the flag which enables the vicarious execution collection device authentication section 32 to read an ID number to the ID attaching part 33 is built in IC card 3, and the IC card authentication section 14 of the vicarious execution collection device 1 will read an ID number from this IC card attaching part 33. Next, the IC card authentication section 14 transmits the contents described by the ID number and transfer-of-fund guarantee demand which were read to the money-value-information Management Department 16. The money-value-information Management Department 16 reduces the amount of money for vicarious execution collection described by the transfer-of-fund guarantee demand from the money value information related with the ID number, and increases only this vicarious execution collected amount to the money value information related with the delivery destination of the amount of money for vicarious execution collection similarly described by the transfer-of-fund guarantee demand. Next, the money-value-information Management Department 16 transmits the contents described by the transfer-of-fund guarantee demand to the transfer-of-fund guarantee creation preserving part 17.

[0048]The transfer-of-fund guarantee creation preserving part 17 draws up a transfer-of-fund guarantee, adds an electronic signature using the secret key which only this vicarious execution collection device 1 can know, and transmits a transfer-of-fund guarantee with this signature to the service provision system 2 via the service provision system communications department 11. The transfer-of-fund guarantee creation preserving part 17 saves this transfer-of-fund guarantee. In the case of this example, the vicarious execution collection device 1 a transfer-of-fund guarantee to the money value information of the delivery destination of the amount of money which carried out vicarious execution collection from the money value information corresponding to IC card 3. It is a bond showing having moved this amount of money for vicarious execution collection, and the delivery destination name of a transfer-of-fund guarantee number, a corresponding transfer-of-fund guarantee demand number, the amount of money for vicarious execution collection, and the amount of money for vicarious execution collection, etc. are described. A transfer-of-fund guarantee number shows the only nature of the published transfer-of-fund guarantee, a transfer-of-fund guarantee demand number shows correspondence with the transfer-of-fund guarantee to publish, the amount of money for vicarious execution collection specifies the amount of money which carries out vicarious execution collection, and the delivery destination name of the amount of money for vicarious execution collection specifies the money value information of the point

which receives the amount of money by which vicarious execution collection was carried out.

[0049]While the vicarious execution collection device 1 saves at drawing 8, an example of the transfer-of-fund guarantee transmitted to the service provision system 2 is shown. Although this descriptive content is fundamentally [as drawing 4] the same, to having been "supplying the following amount of money", by drawing 8, it is "guaranteeing having supplied the following amount of money", and the meanings of a transfer-of-fund guarantee differ at drawing 4.

[0050]The service provision system 2 sends the transfer-of-fund guarantee with a signature sent from the vicarious execution collection device 1 to the transfer-of-fund guarantee management preserving part 25 via the vicarious execution collection device communications department 21. If the electronic signature added to the transfer-of-fund guarantee investigates whether it is what surely was made by the vicarious execution collection device 1 and confirms that it is a just transfer-of-fund guarantee, the transfer-of-fund guarantee management preserving part 25, This transfer-of-fund guarantee is saved, it reports that its service is given to the service provision section 26, and the service provision section 26 gives its service to an IC card owner. When the amount of money for vicarious execution collection is not supplied to the money value information of the delivery destination of the amount of money for vicarious execution collection from the vicarious execution collection device 1, the transfer-of-fund guarantee saved at the service provision system 2 is used in order to require that the amount of money for vicarious execution collection should be supplied to the vicarious execution collection device 1.

[0051]An example of the processing sequence of this example 2 is shown in drawing 9. This is fundamentally [as the processing sequence of previous drawing 5] the same. In the vicarious execution collection center 1, a point of difference from the money value information corresponding to ID received from IC card 3. After subtracting the amount of money for vicarious execution collection indicated to the transfer-of-fund guarantee demand (A15-1), it is only the point that the processing (A15-2) which increases this amount of money for vicarious execution collection to the money value information corresponding to the delivery destination of the amount of money for vicarious execution collection succeeding indicated to the transfer-of-fund guarantee demand is added.

[0052]According to this example 2, what is necessary is just to hold ID to the IC card, and it is not necessary to have money value information. Since the transfer-of-fund guarantee saved at a service provision system is also a bond of movement of monetary value having been performed with a vicarious execution collection device, it does not have money value information. as this effect, the Tampa-proof structure of an IC card is broken, or also when injustice arises in a service provision system, it becomes impossible to increase value creation, i.e., the amount of money, only on a local. A transfer-of-fund guarantee guarantees thoroughly having supplied the amount of money for vicarious execution collection to the delivery destination of the amount of money for vicarious execution collection in exchange for the transfer-of-fund guarantee, and can also prevent the injustice of a vicarious execution collection device, and the dealings and trade managing of a service provision system and a vicarious execution collection device of it about which he can feel easy become possible.

[0053]As mentioned above, although two examples of this invention were described, various modification, such as this invention not being restricted to this and omitting an electronic signature, for example, is possible. Describe the algorithm of a processing sequence as shown in drawing 5 or drawing 9 with the program language which can be performed by computer, for example, it classifies into the object for IC cards, the object for service provision systems, and vicarious execution collection devices, It is also possible to store in the recording media (FD, CD-ROM, etc.) which a computer can read, and to provide. This vicarious execution collection system is realized by installing the program (vicarious execution collection program) of this recording medium in an IC card, a service provision system, and each vicarious execution collection device.

[0054]

[Effect of the Invention]According to the vicarious execution collection system which applied this invention, the following effects are acquired.

(1) Monetary value cannot be put on the local and managed card by which unjust danger is accompanied, and vicarious execution collection can be carried out.

(2) By specifying a thing exchangeable for money, the transfer-of-fund guarantee saved at a service provision system can prevent a third party's injustice, and can improve the safety of the whole system.

(3) Trust establishment of a vicarious execution collection subject and a service provision subject can be made easy, and the injustice of a vicarious execution collection subject and a service provision subject can be prevented.

(4) Compared with the case where the center etc. which carry out batch management of the service provision system are installed, the system which pressed down the communication charges acting as the obstacle of an on-line system can be built.

(5) It will become effective especially with the general-purpose vicarious execution collection service which many service provision subjects can use.

[Translation done.]

6/7

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-148049

(P2001-148049A)

(43) 公開日 平成13年5月29日 (2001.5.29)

(51) Int.Cl. ⁷	識別記号	F I	テームト* (参考)
G 0 7 F 7/12		G 0 6 K 17/00	X 3 E 0 4 4
G 0 6 F 17/60		G 0 7 F 7/10	5 B 0 3 5
	19/00	7/08	C 5 B 0 4 9
G 0 6 K 17/00		G 0 6 F 15/21	3 4 0 A 5 B 0 5 5
	19/10	15/30	M 5 B 0 5 8

審査請求 未請求 請求項の数 7 O L (全 12 頁) 最終頁に続く

(21) 出願番号 特願平11-329083

(22) 出願日 平成11年11月19日 (1999. 11. 19)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 森田 哲之

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(72) 発明者 武藤 信夫

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(74) 代理人 100073760

弁理士 鈴木 誠

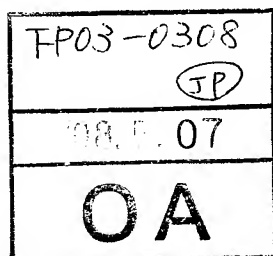
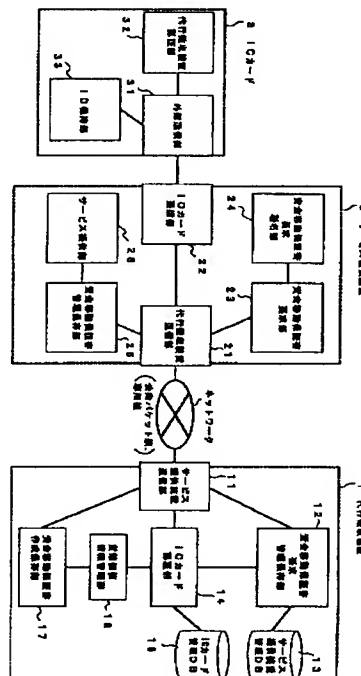
最終頁に続く

(54) 【発明の名称】 代行徴収システム及び代行徴収方法並びに代行徴収プログラムを記録した記録媒体

(57) 【要約】

【課題】 悪意のある者によるローカルでの貨幣価値の創造を意味のないものにし、また、多地点にある複数のサービス提供装置と決済代行センタとの取引を安心して行えるようにする。

【解決手段】 代行徴収装置1は、ICカード3の識別情報 (I D) に関連付けて貨幣価値情報を管理し、ICカード3は該代行徴収装置が管理する貨幣価値情報と関連付けられた当該カード固有のI Dだけを保持し、ローカルに貨幣価値情報を持たない構成とする。サービス提供装置2は、ICカード3が入力されると、代行徴収装置1に対して、代行徴収を行い資金移動保証書の発送を要求する資金移動保証書要求を送信し、代行徴収装置1は、代行徴収した金額を指定の納入先に納入することを保証する資金移動保証書を作成してサービス提供装置2に送信する。



【特許請求の範囲】

【請求項1】 カード利用のサービス提供装置と代行徴収装置がネットワークにより互いに接続され、資金移動保証書要求と資金移動保証書を送受信して、サービス提供装置がサービスするサービス金額を代行徴収装置が代行徴収するシステムであって、

代行徴収装置は、サービス提供装置からの資金移動保証書要求を受信する手段と、カードと相互認証する手段と、カードの識別情報に関連付けて貨幣価値情報を管理する手段と、特定の相手に代行徴収金額を納入することを保証する資金移動保証書を作成しサービス提供装置に送信する手段を具備し、

サービス提供装置は、代行徴収を行い資金移動保証書の発送を要求する資金移動保証書要求を作成して代行徴収装置に送信する手段と、代行徴収装置からの資金移動保証書を受信して管理する手段と、カード利用者にサービスを提供する手段を具備し、

カードは、代行徴収装置が管理する貨幣価値情報と関連付けられた当該カードの識別情報を保持する手段と、代行徴収装置と相互認証する手段を具備する、ことを特徴とする代行徴収システム。

【請求項2】 カード利用のサービス提供装置と代行徴収装置がネットワークにより互いに接続され、資金移動保証書要求と資金移動保証書を送受信して、サービス提供装置がサービスするサービス金額を代行徴収装置が代行徴収するシステムであって、

代行徴収装置は、サービス提供装置からの資金移動保証書要求を受信する手段と、カードと相互認証する手段と、カードの識別情報と代行徴収金額の納入先とに関連付けて貨幣価値情報を管理する手段と、特定の相手に代行徴収金額を納入したことを保証する資金移動保証書を作成しサービス提供装置に送信する手段を具備し、

サービス提供装置は、代行徴収を行い資金移動保証書の発送を要求する資金移動保証書要求を作成して代行徴収装置に送信する手段と、代行徴収装置からの資金移動保証書を受信して管理する手段と、カード利用者にサービスを提供する手段を具備し、

カードは、代行徴収装置が管理する貨幣価値情報と関連付けられた当該カードの識別情報を保持する手段と、代行徴収装置と相互認証する手段を具備する、ことを特徴とする代行徴収システム。

【請求項3】 カード利用のサービス提供装置と代行徴収装置がネットワークにより互いに接続されたシステムにおける代行徴収方法であって、

サービス提供装置は、カード利用者から代行徴収利用を受けると、代行徴収を行い資金移動保証書の発送を要求する資金移動保証書要求を作成して代行徴収装置に送信し、

代行徴収装置は、資金移動保証書要求を受信し、カードと相互認証を行い、相互認証が成功すれば、カードに格

納されている識別情報を取り込み、資金移動保証書要求に記載された代行徴収金額を前記識別情報と関連付けられた貨幣価値情報から減額し、資金移動保証書要求に記載された代行徴収金額納入先に代行徴収金額の納入を保証する資金移動保証書を作成してサービス提供装置に送信し、

サービス提供装置は、代行徴収装置からの資金移動保証書を受信して管理し、カード利用者にサービスを行う、ことを特徴とする代行徴収方法。

10 【請求項4】 カード利用のサービス提供装置と代行徴収装置がネットワークにより互いに接続されたシステムにおける代行徴収方法であって、

サービス提供装置は、カード利用者から代行徴収利用を受けると、代行徴収を行い資金移動保証書の発送を要求する資金移動保証書要求を作成して代行徴収装置に送信し、

代行徴収装置は、資金移動保証書要求を受信し、カードと相互認証を行い、相互認証が成功すれば、カードに格納されている識別情報を取り込み、資金移動保証書要求に記載された代行徴収金額を前記識別情報と関連付けられた貨幣価値情報から減額し、資金移動保証書要求に記載された代行徴収金額納入先に関連付けられた貨幣価値情報に増額し、資金移動保証書要求に記載された代行徴収金額納入先に代行徴収金額の納入済みを保証する資金移動保証書を作成してサービス提供装置に送信し、サービス提供装置は、代行徴収装置からの資金移動保証書を受信して管理し、カード利用者にサービスを行う、ことを特徴とする代行徴収方法。

30 【請求項5】 請求項3又は4記載の代行徴収方法において、

代行徴収装置は、資金移動保証書に当該代行徴収装置の電子署名を付加してサービス提供装置に送信し、

サービス提供装置は、資金移動保証書の電子署名を検査し、正しい署名であれば、該資金移動保証書を保存し、サービスを行う、ことを特徴とする代行徴収方法。

【請求項6】 請求項3、4又は5記載の代行徴収方法において、

サービス提供装置は、資金移動保証書要求に当該サービス提供装置の電子署名を付加して代行徴収装置に送信し、

代行徴収装置は、資金移動保証書要求の電子署名を検査し、正しい署名であれば、該資金移動保証書要求を保存し、カードと相互認証を行う、ことを特徴とする代行徴収方法。

【請求項7】 請求項3、4、5又は6記載の代行徴収方法の処理を、コンピュータで実行させるための代行徴収プログラムを格納したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ＩＣカード等を利用した代行徴収システム及びその方法並びに代行徴収プログラムを記録した記録媒体に関する。

【０００２】

【従来の技術】一般にカードを利用した代行徴収システムは、貨幣価値を管理する場所によって、共通バスカードなどのようにカードの中に貨幣価値を持つ種類のシステム（以下、前者）と、センタが貨幣価値を管理し、利用者はセンタに対してＩＤ（ＩＤ：Identifier）などの識別情報を伝えることで、センタ内の貨幣価値を操作して代行徴収を行う種類のシステム（以下、後者）との、二つに分類される。ここでいう貨幣価値とは、それ自身が貨幣となりうるものであり、たとえば電子マネーのデータである。

【０００３】前者は、代行徴収を依頼する利用者が所有するカードの中に貨幣価値情報を電子的に記録し、その貨幣価値情報をサービス提供装置が読み取ることによって、ローカルでの決済を可能にするシステムである。本システムとしては共通バスカードのほかにも、Ｕカード、クオカードなど現在広く流通しているプリペイド型の代行徴収システムが挙げられる。しかし、ローカルにあるカードの中に貨幣価値情報を持つ代行徴収システムでは、電子価値の創造がローカルで行われる可能性がある。また、パチンコカードに代表されるように、代行徴収業者が代行徴収を行うシステムでは、利用者個人ではなく、代行徴収システムに代行徴収を依頼する業者が容易に偽造電子価値によって現金を得るというシステムになり、組織ぐるみの犯罪が、ネットワークでつながっていない場所、つまり代行徴収業者からは直接わからない場所で行われるという危険があった。

【０００４】後者は、代行徴収センタが代行徴収を依頼する利用者の全貨幣価値情報を一箇所で一元管理する代行徴収システムである。利用者は決済代行センタが管理する貨幣価値情報との関連づけがなされたＩＤをもち、利用者は決済センタにＩＤを含む代行徴収依頼の情報を通知することにより、代行徴収センタは代行徴収センタ内の貨幣価値情報を変化させ、依頼された先へ決済額を納入する。よって、貨幣価値情報はセンタの外に出ることは無く、ローカルでの貨幣価値創造はなされないという利点がある。

【０００５】従来、このセンタ型のシステムには、例えばインターネット上で利用されているアコシスがある。アコシスの場合、代行徴収センタは利用者からの代行徴収の依頼のたびに、販売業者のホストと通信をおこなって代行徴収を行うことを通知し、販売業者のホストは該通知を受けると利用者に対してサービスを行う。該ホストは一箇所にあるため、販売業者は代行徴収センタとの取引及び取引の管理が容易であり、徴収代行後、確実に販売業者へお金が支払われ、決済業者と販売業者間の信頼関係の確立は、単なる取引データの通知という手段で

可能であり、容易であった。

【０００６】しかし、自動販売機のような、複数あるサービス提供装置が多地点に分かれて存在する場合、販売業者と代行徴収業者との取引及び取引の管理は難しい。よって、悪意ある販売業者あるいは悪意ある決済代行業者の不正も考えられ、従来の単なる取引データの通知という手段では、販売業者と代行徴収業者との信頼ある取引が難しかった。取引管理手段として、代行徴収センタと複数のサービス提供装置との取引を販売業者の一つのホストを通して行うことで、取引管理を販売業者のホストが集中管理する方式も考えられるが、これは通信コストがかかるという問題がある。

【０００７】

【発明が解決しようとする課題】本発明の目的は、カードを利用した代行徴収システムにおいて、悪意のある者によるローカルでの貨幣価値の創造を不可あるいは意味のないものとするとともに、多地点に複数あるサービス提供装置と決済代行センタとの取引を安心して行え、また通信コストを抑えることにある。

【０００８】

【課題を解決するための手段】本発明は、代行徴収を行う代行徴収装置が、多地点に複数あるサービス提供装置と不正のない取引を行うことを可能とするため、サービス提供装置が資金移動保証書要求を代行徴収装置に送信し、代行徴収装置が代行徴収した金額を指定の納入先との間で貨幣価値と交換する資金移動保証書を作成してサービス提供装置に送信し、サービス提供装置は該資金移動保証書を保存することを最も大きな特徴とする。従来の技術とは、ローカルに貨幣価値情報を持たないセンタ管理型のシステム、資金移動保証書を用いた代行徴収システムとすることで、多地点にあるサービス提供装置との不正のない安心できる取引を可能にすることが異なる。

【０００９】本発明の代行徴収システムでは、代行徴収利用者の貨幣価値情報を管理する代行徴収装置と、複数のサービス提供装置と、代行徴収装置の貨幣価値情報と関連付けられた識別情報（ＩＤ：Identifier）を格納できるＩＣカード等で構成される。本発明では、ＩＣカード所有者は貨幣価値情報と関連付けられたＩＣカードをすでに所有しており、ＩＣカード所有者は代行徴収装置にある貨幣価値情報に入金しているとする。

【００１０】代行徴収装置は、ＩＣカード認証手段と貨幣価値情報管理手段と資金移動保証書作成手段と電子署名手段などを備えている。資金移動保証書には、資金移動保証書識別子と代行徴収金額と代行徴収金額の納入先名などが記述され、さらに代行徴収主体の電子署名が付加される。該資金移動保証書は、代行徴収装置が資金移動保証書要求と引き換えに代行徴収した金額の納入先に金額を渡すことを保証するものであると定義する。資金移動保証書識別子はすべての資金移動保証書のなかで唯

一のもの（例えば通し番号）とすることで、資金移動保証書の唯一性を保証する効果がある。代行徴収金額は代行徴収する金額を特定する効果があり、代行徴収金額の納入先名は社会的にみて唯一なものに対応づけされる名前にすることにより、代行徴収金額の渡し先を特定するものであり、これにより第3者による資金移動保証書を複製する意味を無くし、不正を防止する効果がある。

【0011】サービス提供装置は、資金移動保証書要求手段と資金移動保証書管理保存手段とサービス提供手段などを備えている。資金移動保証書要求とは、代行徴収金額と代行徴収金額の納入先が記述された資金移動保証書をサービス提供装置に送信するよう要求する命令であると定義する。代行徴収金額は代行徴収される金額を指定する効果があり、代行徴収金額の納入先は代行徴収装置が資金移動保証書と貨幣価値を交換する相手を特定する効果がある。

【0012】ＩＣカードは、ＩＤ保持手段と代行徴収装置との認証手段などを備えて構成される。ＩＤは代行徴収装置の貨幣価値情報と関連付けられた識別情報（Identifier）である。ＩＣカードとは、代行徴収装置と相互認証でき、また、代行徴収装置以外がＩＤを改ざんできない構成の、利用者が持ち運びできるものと定義する。なお、本発明では、同様の構成のものであれば、一般に任意のカードが利用可能である。

【0013】代行徴収利用者は、代行徴収装置の貨幣価値情報と関連付けられたＩＣカードを持つ。ＩＣカードを持つ利用者がサービス提供装置にＩＣカードを入力し代行徴収利用意志を伝え、サービス提供装置は資金移動保証書要求を作成し、代行徴収装置に送信する。代行徴収装置は、サービス提供装置から資金移動保証書要求を受け取ると、まず、サービス提供装置に入力されたＩＣカードと相互認証を行い、ＩＣカードからＩＤを読み取る。次に、代行徴収装置は、読み取ったＩＤに関連する貨幣価値情報をさがし、資金移動保証書要求で要求された金額を減額する。次に、代行徴収装置は、資金移動保証書を作成し、代行徴収装置のみが知り得る情報を用いて資金移動保証書に電子署名を付加し、該資金移動保証書をサービス提供装置に送信する。サービス提供装置は、資金移動保証書を受け取ると、資金移動保証書の内容と署名が正しいものかを調べ、正しければ、資金移動保証書を保存する。その後、サービス提供装置は代行徴収利用者に対してサービスを行う。また、保存された資金移動保証書は何らかの形で資金移動保証書に記載された代行徴収金額の納入先に渡され、代行徴収金額の納入先は代行徴収装置との間で、資金移動保証書を現金に代表される貨幣価値と交換する。

【0014】本代行徴収システムによると、サービス提供装置は代行徴収装置と事前の契約無しに安心して代行徴収を利用することが出来る。これは貨幣価値である資金移動保証書をそれぞれのサービス提供装置が直接、代

行徴収装置から受け取ることによるものである。

【0015】本発明の別の態様においては、代行徴収装置は代行徴収金額の納入先の貨幣価値情報を持ち、サービス提供装置から資金移動保証書要求を受けて、代行徴収金額をＩＣカードに関連付けられた貨幣価値情報から減額して代行徴収金額の納入先の貨幣価値情報に移す。この場合、資金移動保証書は、代行徴収装置がＩＣカードに対応した貨幣価値情報から代行徴収した金額の納入先の貨幣価値情報へ代行徴収金額を移動したことを表す証書であると定義する。サービス提供装置に保存された資金移動保証書は、代行徴収装置から代行徴収金額の納入先の貨幣価値情報に代行徴収金額が納入されない代行徴収装置の不正を防ぐ効果がある。

【0016】本態様によると、貨幣価値を代行徴収装置の外で扱う必要が無く、ローカルでの価値の創造は不可能となる効果がある。

【0017】また、本発明の別の態様においては、サービス提供装置は資金移動保証書要求にサービス提供装置のみが知りうる情報を用いて署名する手段を持ち、資金移動保証書要求にはサービス提供装置のみが知りうる情報を用いた署名が添付される。代行徴収装置は、資金移動保証書要求の署名を検査し、正しい署名であれば、該資金移動保証書要求を保存し、ＩＣカードとの相互認証を開始する。

【0018】

【発明の実施の形態】以下、図面を用いて、本発明の一実施の形態について詳細に説明する。

【0019】〔実施例１〕図１は、本実施例１が適用される代行徴収システムの全体的構成例を示したものである。図１において、１は代行徴収を行う代行徴収装置、２は多地点に複数存在するサービス提供装置、３は利用者が所有するＩＣカードである。

【0020】代行徴収装置１は、サービス提供装置２とネットワーク（公衆パケット網、専用線など）を介して通信を行うサービス提供装置通信部１１と（これはモデムなどが代表される）、資金移動保証書要求を管理し保存する資金移動保証書要求管理保存部１２と、各サービス提供装置２の公開鍵等を保持するサービス提供装置管理データベース（サービス提供装置管理ＤＢ）１３と、ＩＣカード３と相互認証を行うＩＣカード認証部１４と、ＩＣカード３と相互認証を行うための各ＩＣカード対応の共通鍵等を保持するＩＣカードデータベース（ＩＣカードＤＢ）１５と、ＩＣカード３に格納されたＩＤ番号と関連付けられた貨幣価値情報を管理する貨幣価値情報管理部１６と、資金移動保証書を作成し当該代行徴収装置１の署名を付加する資金移動保証書作成保存部１７とで構成される。

【0021】図２に、代行徴収装置１の貨幣価値情報管理部１６が管理する貨幣価値情報の一例を示す。図２において、例えばＩＣカードに格納されたＩＤ番号「００

「001」に対応する貨幣価値情報である現金預かり金額は20000円であることを示している。ID番号「00002」、「00003」についても同様である。各ICカード所有者は、あらかじめ所定の金額を入金しておく。

【0022】サービス提供装置2は、代行徴収装置1と通信を行う代行徴収装置通信部21と、ICカード3と通信を行うICカードリード・ライト(R/W)で代表されるICカード通信部22と、代行徴収利用の意志をICカード所有者から受け付け、資金移動保証書要求を作成する資金移動保証書要求部23と、資金移動保証書要求に当該サービス提供装置の署名を付加する資金移動保証書要求署名部24と、代行徴収装置1から送られる資金移動保証書を記録し保存する資金移動保証書管理保存部25と、代行徴収利用者に実際にサービスを行うサービス提供部26とで構成される。

【0023】ICカード3は、サービス提供装置2と通信を行う外部通信部31と代行徴収装置1と相互認証を行う代行徴収装置認証部32と、代行徴収装置1の貨幣価値情報と関連付けられたID番号を保持するID保持部33とで構成される。

【0024】代行徴収装置1において、サービス提供装置通信部11は資金移動保証書要求管理保存部12及びICカード認証部14及び資金移動保証書作成保存部17とネットワークを介したサービス提供装置2との通信を中継する。資金移動保証書要求管理保存部12はサービス提供装置管理DB13とICカード認証部14と通信する。ICカード認証部14は更にICカード管理DB15と貨幣価値情報管理部16と通信する。貨幣価値情報管理部16は更に資金移動保証書作成保存部17と通信する。

【0025】サービス提供装置2において、代行徴収装置通信部21は資金移動保証書要求部23及び資金移動保証書管理保存部25とネットワークを介した代行徴収装置1との通信を中継する。ICカード通信部22はICカード3と通信を行い、必要ならば代行徴収装置通信部21を介して代行徴収装置1とICカード3との通信を中継する。資金移動保証書要求部23は更に資金移動保証書要求署名部24と通信する。資金移動保証書管理保存部25は更にサービス提供部26と通信する。

【0026】ICカード3において、外部通信部31は代行徴収装置認証部32及びID保持部33とサービス提供装置2を介した代行徴収装置1との通信を中継する。

【0027】次に、本実施例の動作を説明する。利用者は、ICカード3をサービス提供装置2に入力するなどして、代行徴収利用の意志を行う。サービス提供装置2は、ICカード通信部22、代行徴収装置通信部21を介して、ICカード所有者から代行徴収利用の意志を資金移動保証書要求部23が受け取ると、資金移動保証書

要求部23は資金移動保証書要求を作成する。資金移動保証書要求には、サービス提供装置名と代行徴収の金額と代行徴収金額の納入先名と資金移動保証書要求番号と資金移動保証書要求の作成日時と当該サービス提供装置2のネットワークアドレスなどが記述される。サービス提供装置名は代行徴収を要求する装置を特定する効果があり、代行徴収金額は代行徴収される金額を指定する効果がある。代行徴収金額の納入先は代行徴収装置1が資金移動保証書と引き換えに現金と渡す先を特定する効果があり、第3者の資金移動保証書を盗用する意味を無くして資金移動保証書の盗難を防止する効果がある。資金移動保証書要求番号は、サービス提供装置によって一度だけ用いられる識別子であり、該資金移動保証書要求番号と作成日時によって、資金移動保証書要求を唯一なものに特定する効果がある。サービス提供装置のネットワークアドレスはサービス提供装置2のネットワーク上の場所を通知する効果がある。

【0028】次に、資金移動保証書要求部23は、資金移動保証書要求署名部24に対して作成した資金移動保証書要求を送信し、資金移動保証書要求署名部24は、資金移動保証書要求に対して当該サービス提供装置2のみが知り得る秘密鍵を用いて電子署名を付加し、改ざんと成り済ましを防止すると、資金移動保証書要求部23に返す。該電子署名により資金移動保証書要求を作成したサービス提供装置を特定することは、ICカードが利用されたサービス提供装置を分析してICカード利用者の利用動向をつかむなどの情報収集に役立つだけでなく、万が一不正が行われた場合に、不正追跡のための一情報となる効果がある。

【0029】サービス提供装置2は、資金移動保証書要求部23に返された署名付きの資金移動保証書要求を、代行徴収装置通信部21を介して代行徴収装置1に送信する。図3に、代行徴収装置1に送信される資金移動保証書要求の一例を示す。

【0030】代行徴収装置1は、サービス提供装置2からの署名付き資金移動保証書要求をサービス提供装置通信部11が受信し、資金移動保証書要求管理保存部12に送る。資金移動保証書要求管理保存部12は、サービス提供装置管理DB13に保持しているサービス提供装置2の公開鍵を用いて資金移動保証書要求の電子署名を検査し、正しい署名であると判断すると、該資金移動保証書要求を保存し、また、ICカード認証部14に資金移動保証書要求に記述された内容を通知する。保存された資金移動保証書要求は、サービス提供装置2が確かに当該代行徴収装置1に対して代行徴収を依頼したという証拠となる効果がある。

【0031】次に、ICカード認証部14は、ICカード管理DB15に保持されている。共通鍵を用い、資金移動保証書要求に記述されたサービス提供装置2のネットワークアドレスを元に、サービス提供装置通信部1

1、サービス提供装置2の代行徴収装置通信部21及びICカード通信部22、ICカード3の外部通信部31を介して、ICカード3の代行徴収装置認証部32と相互認証を行う。相互認証とは、二者が互いに相手あるいは限られた者のみが知りうる秘密情報を持っていることを確認して、互いに相手が誰であるかを判断する処理である。例えば、共通鍵を用いたチャレンジレスポンス方式が一般的である。相互認証が成功すると、ICカード3は、代行徴収装置認証部32がID保持部33に対してID番号を読み出すことを可能にするフラグをたてるよう通知し、ICカード認証部14は、該ICカード3のICカード保持部33からID番号を読み込む。その後、ICカード認証部14は、読み込んだID番号及び資金移動保証書要求に記述された内容を貨幣価値情報管理部16に送る。貨幣価値情報管理部16は、資金移動保証書要求に記載された代行徴収金額をID番号に関連付けられた貨幣価値情報から減額し、資金移動保証書要求に記述された内容を資金移動保証書作成保存部17に送る。

【0032】資金移動保証書作成保存部17は資金移動保証書を作成し、該代行徴収装置1のみが知りうる秘密鍵を用いて電子署名を付加し、サービス提供装置通信部11を介してサービス提供装置2に送信する。また、資金移動保証書作成保存部17は、該資金移動保証書を保存する。資金移動保証書は、資金移動保証書番号と対応する資金移動保証書要求番号と、代行徴収金額と、代行徴収金額の納入先名などが記述される。資金移動保証書は、代行徴収装置1が該資金移動保証書と引き換えに代行徴収した金額の納入先に金額を渡すことを保証する貨幣価値であり、資金移動保証書番号は発行された資金移動保証書の唯一性を示す効果があり、資金移動保証書要求番号は発行する資金移動保証書との対応をとる効果があり、代行徴収金額は代行徴収する金額を特定する効果があり、代行徴収金額の納入先名は代行徴収された金額を受け取ることが出来る先を特定する効果がある。

【0033】図4に、代行徴収装置1が保存するとともにサービス提供装置2に送信される資金移動保証書の一例を示す。これは、図3の資金移動保証書要求に対応して発行される資金移動保証書を示している。

【0034】サービス提供装置2は、代行徴収装置1から送られた電子署名付きの資金移動保証書を代行徴収装置通信部21が受信して資金移動保証書管理保存部25に送る。資金移動保証書管理保存部25は、資金移動保証書に付加された電子署名が確かに代行徴収装置1によってなされたものかを調べ、正当な資金移動保証書であることを確かめると、該資金移動保証書を保存し、サービス提供部26にサービスを行うように通知し、サービス提供部26は、ICカード所有者に対してサービスを行う。なお、保存された資金移動保証書は、該資金移動保証書に記載された代行徴収金額の納入先に渡され、代

行徴収金額の納入先は代行徴収装置1との間で、資金移動保証書と現金を交換することになる。

【0035】図1のシステムによれば、ICカード3には、代行徴収装置1が管理する貨幣価値情報と関連付けられたIDを保持しているだけでよく、貨幣価値情報を持つ必要がない。この効果としては、ICカードの耐タンパ構造が破られてもローカルだけで価値創造つまり金額を増やすこと等は不可能となる。また、サービス提供装置2に保存される資金移動保証書は代行徴収金額の納入先と金額が固定されているため、第3者が不正を行っても該第3者が利益を得る構造とはならず、第3者の不正を防止できる。資金移動保証書はその唯一性を資金移動保証書番号によって保証されているので、代行徴収金額の納入先も資金移動保証書を複製して利益を得ることは不可能である。また、資金移動保証書は該資金移動保証書と引き換えに代行徴収金額の納入先へ代行徴収金額を渡すことを完全に保証するものであり、代行徴収装置1の不正も防止でき、サービス提供装置2と代行徴収装置1との安心できる取引及び取引管理が可能となる。

【0036】図5に、本実施例の処理シーケンスの一例を示す。これは、ICカード3の所有者がすでに代行徴収装置1に現金を払い、代行徴収装置1は該ICカード3に対応した貨幣価値情報に受け取った現金額を増額済みであるという状況のもとで、ICカード所有者によって代行徴収の利用意志を受けたサービス提供装置2が代行徴収装置1と通信して代行徴収を依頼し、代行徴収装置1から資金移動保証書を受け取りサービスを行うまでの、実施例1の処理シーケンスを示したものである。ここでは、代行徴収装置1として代行徴収センタ、サービス提供装置2としてジュースの自動販売機、サービスとして缶ジュースの販売を例にする。

【0037】ICカード所有者はICカード3を自動販売機2に挿入して、所望の缶ジュースのボタンを押し、自動販売機2に代行徴収の利用意志を通知する(S11)。自動販売機2は、代行徴収センタ1に対して代行徴収を行うように要求する資金移動保証書要求を作成する(S12)。資金移動保証書要求には、自動販売機名と代行徴収の金額と代行徴収金額の納入先名と資金移動保証書要求番号と資金移動保証書要求の作成日時と自動販売機2のネットワークアドレスなどが記述される。自動販売機名は代行徴収を要求する装置を特定し、代行徴収金額は代行徴収される缶ジュースの金額を指定する。代行徴収金額の納入先は代行徴収センタ1が資金移動保証書と引き換えに現金と渡す先を特定するため、第3者の資金移動保証書を盗用する意味を無くして資金移動保証書の盗難を防止できる。また、資金移動保証書要求番号を自動販売機によって1度だけ用いられる識別子とすることで、資金移動保証書要求番号と作成日時は資金移動保証書要求を唯一なものに特定できる。自動販売機のネットワークアドレスは自動販売機2のネットワーク上

の場所を通知する。自動販売機2は、資金移動保証書要求に対して当該自動販売機2のみが知りうる秘密鍵で電子署名を付加し（S13）、該署名付き資金移動保証書要求を代行徴収センタ1に送信する（S14）。

【0038】代行徴収センタ1は、受け取った資金移動保証書要求の電子署名が確かに自動販売機2のものであり、また資金移動保証書要求が改ざんされていないことを確認すると（A11）、該資金移動保証書要求を保存する（A12）。保存された資金移動保証書要求は、事後トラブル時などに、確かに自動販売機2が代行徴収を代行徴収センタ1に依頼したという証拠となる。次に、代行徴収センタ1は、ICカード3と相互認証を行う（A13、I11）。相互認証は、共通鍵を用いたチャレンジレスポンス方式などで行い、ICカード3と認証装置1以外の例えば自動販売機2などでは解読したり模倣することが出来ない方式で行う。相互認証が成功すると、ICカード3は該ICカードに格納されたIDを読み取り可能にし、代行徴収センタ1はICカード3に対してIDの読み取りを要求し（A14）、ICカード3はIDを代行徴収センタ1に通知する（I12）。

【0039】代行徴収センタ1は、ICカード3から受け取ったIDに対応する貨幣価値情報から、資金移動保証書要求に記載された金額を減額する（A15）。次に、代行徴収センタ1は資金移動保証書を作成する（A16）。資金移動保証書は、代行徴収センタ1が資金移動保証書と引き換えに代行徴収金額の納入先に上記金額を渡すことを保証する貨幣価値であり、資金移動保証書番号と、対応する資金移動保証書要求番号と、代行徴収金額と、代行徴収金額の納入先名などが記述される。資金移動保証書番号は発行された資金移動保証書の唯一性を示し、資金移動保証書要求番号は発行する資金移動保証書との対応をとるものである。代行徴収金額は代行徴収する金額を特定し、代行徴収金額の納入先名は代行徴収された金額を受け取ることができる先を特定する。次に、代行徴収センタ1は資金移動保証書に当該代行徴収センタ1のみが知りうる秘密鍵を用いて電子署名を付加し、改ざん、成り済ましを防止した後（A17）、該署名付き資金移動保証書を自動販売機2に送信する（A18）。

【0040】自動販売機2は、代行徴収センタ1から資金移動保証書を受け取ると、該資金移動保証書の電子署名をチェックし（S15）、資金移動保証書に記載されている内容が資金移動保証書要求で要求した内容と合致するかを調べ（S16）、正常であれば該資金移動保証書を保存し（S17）、ICカード所有者に対して缶ジュースを提供する（S18）。その後、保存された資金移動保証書は、該資金移動保証書に記載された代行徴収金額の納入先に渡され、代行徴収金額の納入先は代行徴収センタ1との間で、資金移動保証書と現金を交換することになる。

【0041】図5の処理シーケンスによれば、自動販売機2と代行徴収センタ1との通信は、ICカード3との通信時を除けば、資金移動保証書要求を自動販売機2から代行徴収センタ1に送信する時と、資金移動保証書を代行徴収センタ1から自動販売機2に送信する時との2度に限られ、例えば自動販売機を集中管理するセンタを別に設置し、該センタを通して、自動販売機と代行徴収センタとの取引を行う場合より、明らかに通信回数が軽減される事がわかる。

【0042】〔実施例2〕本実施例は、代行徴収装置が代行徴収金額の納入先の貨幣価値情報を持ち、サービス提供装置から資金移動保証書要求を受けて、代行徴収金額をICカードに関連付けられた貨幣価値情報から代行徴収金額の納入先の貨幣価値情報に移すものである。本実施例では、資金移動保証書の持つ意義が、先の実施例1の場合と異なる。即ち、実施例1では、資金移動保証書が代行徴収金額の納入先に渡されて、該代行徴収金額の納入先が代行徴収装置との間で資金移動保証書と現金を交換するため、資金移動保証書は貨幣価値を持った。これに対して、本実施例の場合、代行徴収装置内で貨幣価値情報の移動が完了するため、資金移動保証書は、貨幣価値を持たないが、貨幣価値が移動したという証拠となる証書（支取済み証書）としての意味を持つ。

【0043】本実施例の全体的なシステム構成は、図1と基本的に同様であるので省略する。ただし、代行徴収装置1内の貨幣価値情報管理部16は、ICカード3に格納されたID番号と関連付けられた貨幣価値情報に加えて、代行徴収金額の納入先と関連付けられた貨幣価値情報を管理する。図6に、本実施例において貨幣価値情報管理部16が管理する貨幣価値情報の一例を示す。ここで、「ABC株式会社」、「DEF株式会社」、「日本 太郎」などが代行徴収金額の納入先名を示している。ただ、IDが納入先、上記会社名や個人名が納入元となることも可能である。

【0044】次に、図1のシステム構成により、本実施例2の動作を説明する。利用者は、ICカード3をサービス提供装置2に入力するなどして、代行徴収利用の意志を行う。サービス提供装置2では、システムICカード所有者からの代行徴収利用の意志を資金移動保証書要求部23が受け取り、資金移動保証書要求を作成する。資金移動保証書要求には、サービス提供装置名と代行徴収の金額と代行徴収金額の納入先名と資金移動保証書要求番号と資金移動保証書要求の作成日時と当該サービス提供装置2のネットワークアドレスなどが記述される。本実施例の場合、資金移動保証書要求は、サービス提供装置2が代行徴収装置1に対して、代行徴収金額をICカード3に関連付けられた貨幣価値情報から該納入先に関連付けられた貨幣価値情報に納入するよう依頼する意味を持つ。即ち、資金移動保証書要求内の代行徴収金額の納入先は、代行徴収装置1が該資金移動保証書要求

を受けて代行徴収金額を納入する先の貨幣価値情報を特定する意味を持つ。資金移動保証書要求内のほかの記述内容が持つ意味は、先の実施例1の場合と基本的に同じである。資金移動保証書要求部23は、作成した資金移動保証書要求を資金移動保証書要求署名部24に送り、資金移動保証書要求署名部24は資金移動保証書要求に対して当該サービス提供装置2のみが知り得る秘密鍵を用いて電子署名を付加し、資金移動保証書要求部23に返す。

【0045】サービス提供装置2は、資金移動保証書要求部23に返された当該サービス提供装置2の署名付き資金移動保証書要求を、代行徴収装置通信部21を介して代行徴収装置1に送信する。図7に、代行徴収装置1に送信される資金移動保証書要求の一例を示す。これは図3の内容と基本的に同様である。

【0046】代行徴収装置1は、サービス提供装置2からの署名付き資金移動保証書をサービス提供装置通信部11を通して資金移動保証書要求管理保存部12に送る。資金移動保証書要求管理保存部12は、サービス提供装置管理DB13に保持しているサービス提供装置2の公開鍵を用いて資金移動保証書要求の電子署名を検査し、正しい署名であると判断すると、該資金移動保証書要求を保存し、また、ICカード認証部14に資金移動保証書要求に記述された内容を通知する。保存された資金移動保証書要求は、サービス提供装置2が確かに代行徴収装置1に対して代行徴収を依頼したという証拠となる。

【0047】ICカード認証部14は、ICカード管理部15に保持されている共通鍵を用いてチャレンジレスポンス方式などで、資金移動保証書要求に記述されたサービス提供装置2のネットワークアドレスを元に、サービス提供装置通信部11ー代行徴収装置通信部21ーICカード通信部22ー外部通信部31を介して、ICカード3の代行徴収装置認証部32と相互認証を行う。相互認証が成功すると、ICカード3では、代行徴収装置認証部32がID保持部33にID番号を読み出すことを可能にするフラグをたてるよう通知し、代行徴収装置1のICカード認証部14は該ICカード保持部33からID番号を読み込む。次に、ICカード認証部14は読み込んだID番号及び資金移動保証書要求に記述された内容を貨幣価値情報管理部16に送信する。貨幣価値情報管理部16は、資金移動保証書要求に記述された代行徴収金額をID番号に関連付けられた貨幣価値情報から減額し、同じく資金移動保証書要求に記述された代行徴収金額の納入先に関連付けられた貨幣価値情報に該代行徴収額だけ増額する。次に、貨幣価値情報管理部16は資金移動保証書要求に記述された内容を資金移動保証書作成保存部17に送信する。

【0048】資金移動保証書作成保存部17は資金移動保証書を作成し、該代行徴収装置1のみが知りうる秘密

鍵を用いて電子署名を付加し、該署名付きの資金移動保証書を、サービス提供装置通信部11を介してサービス提供装置2に送信する。また、資金移動保証書作成保存部17は、該資金移動保証書を保存する。本実施例の場合、資金移動保証書は、代行徴収装置1がICカード3に対応した貨幣価値情報から代行徴収した金額の納入先の貨幣価値情報へ、該代行徴収金額を移動したことを表す証書であり、資金移動保証書番号と対応する資金移動保証書要求番号と、代行徴収金額と、代行徴収金額の納入先名などが記述される。資金移動保証書番号は発行された資金移動保証書の唯一性を示し、資金移動保証書要求番号は発行する資金移動保証書との対応を示し、代行徴収金額は代行徴収する金額を特定し、代行徴収金額の納入先名は代行徴収された金額を受け取る先の貨幣価値情報を特定する。

【0049】図8に、代行徴収装置1が保存するとともにサービス提供装置2に送信される資金移動保証書の一例を示す。この記述内容は、図4と基本的に同様であるが、図4では「以下の金額を納入する」であったのに対し、図8では「以下の金額を納入したことを保証する」であり、資金移動保証書の意味が異なる。

【0050】サービス提供装置2は、代行徴収装置1から送られた署名付きの資金移動保証書を代行徴収装置通信部21を介して資金移動保証書管理保存部25に送る。資金移動保証書管理保存部25は、資金移動保証書に付加された電子署名が確かに代行徴収装置1によってなされたものかを調べ、正当な資金移動保証書であることを確かめると、該資金移動保証書を保存し、サービス提供部26にサービスを行うように通知し、サービス提供部26はICカード所有者に対してサービスを行う。なお、サービス提供装置2に保存された資金移動保証書は、代行徴収装置1から代行徴収金額の納入先の貨幣価値情報に代行徴収金額が納入されない場合に、代行徴収装置1に対して代行徴収金額を納入するよう要求するために利用する。

【0051】図9に、本実施例2の処理シーケンスの一例を示す。これは、先の図5の処理シーケンスと基本的に同様である。相違点は、代行徴収センタ1において、ICカード3から受け取ったIDに対応する貨幣価値情報から、資金移動保証書要求に記載された代行徴収金額を減算した後(A15-1)、引き続き資金移動保証書要求に記載された代行徴収金額の納入先に対応する貨幣価値情報に、該代行徴収金額を増額する処理(A15-2)が追加されている点だけである。

【0052】本実施例2によれば、ICカードにはIDを保持しているだけでよく、貨幣価値情報を持つ必要がない。また、サービス提供装置に保存される資金移動保証書も代行徴収装置で貨幣価値の移動が行われたことの証書であるので、貨幣価値情報は持たない。この効果としては、ICカードの耐タンパ構造が破られるあるいは

10

20

30

40

50

サービス提供装置に不正が生じた場合にもローカルだけで価値創造つまり金額を増やすことは不可能となる。また、資金移動保証書は資金移動保証書と引き換えに代行徴収金額の納入先へ代行徴収金額を納入したことを完全に保証するものであり、代行徴収装置の不正も防止でき、サービス提供装置と代行徴収装置との安心できる取引及び取引管理が可能となる。

【0053】以上、本発明の二つの実施例について説明したが、本発明はこれに限られるものではなく、例えば電子署名は省略するなど、種々の変形が可能である。また、図5や図9に示したような処理シーケンスのアルゴリズムをコンピュータで実行可能なプログラム言語で記述し、例えば、ICカード用、サービス提供装置用、代行徴収装置用に区分して、コンピュータが読み取り可能な記録媒体（FD、CD-ROM等）に格納して提供することも可能である。この記録媒体のプログラム（代行徴収プログラム）をICカード、サービス提供装置、代行徴収装置それぞれにインストールすることにより、本代行徴収システムが実現する。

【0054】

【発明の効果】本発明を適用した代行徴収システムによれば次のような効果が得られる。

（1）不正の危険の伴うローカルで管理されるカードに貨幣価値を置くことがなく、代行徴収することができる。

（2）サービス提供装置に保存される資金移動保証書はお金と交換できるものを特定することによって、第三者の不正を防止し、システム全体の安全性を高めることができる。

（3）代行徴収主体とサービス提供主体の信用確立を容易にし、代行徴収主体およびサービス提供主体の不正を防止することができる。

（4）サービス提供装置を一括管理するセンタ等を設置する場合に比べて、オンラインシステムの障害となる通信費を押さえたシステムが構築できる。

（5）多くのサービス提供主体が利用できる汎用代行徴収サービスで特に有効なものとなる。

【図面の簡単な説明】

【図1】本発明が適用されるシステムの構成例を示す図である。

【図2】代行徴収装置が管理する貨幣価値情報の一例を示す図である。

【図3】資金移動保証書要求の一例を示す図である。

【図4】資金移動保証書の一例を示す図である。

【図5】本発明が提供されるシステムの処理シーケンスの一例を示す図である。

【図6】代行徴収装置が管理する貨幣価値情報の他の一例を示す図である。

【図7】資金移動保証書要求の他の一例を示す図である。

【図8】資金移動保証書の他の一例を示す図である。

【図9】本発明が提供されるシステムの処理シーケンスの他の一例を示す図である。

【符号の説明】

- 1 代行徴収装置
- 2 サービス提供装置
- 3 ICカード
 - 11 サービス提供装置通信部
 - 12 資金移動保証書要求管理保存部
 - 13 サービス提供装置管理DB
 - 14 ICカード認証部
 - 15 ICカード管理DB
 - 16 貨幣価値情報管理部
 - 17 資金移動保証書作成保存部
- 21 代行徴収装置通信部
- 22 ICカード通信部
- 23 資金移動保証書要求部
- 24 資金移動保証書要求署名部
- 25 資金移動保証書管理保存部
- 26 サービス提供部
- 31 外部通信部
- 32 代行徴収装置認証部
- 33 ID保持部

【図3】

資金移動保証書要求

代行徴収を行うことを要求する

資金移動保証書要求番号：ABC001

サービス提供装置名：ABC株式会社1番機

作成日時：1999/02/05/12:45:09

代行徴収金額：1000円

代行徴収金額納入先名：ABC株式会社

サービス提供装置IPアドレス：129.0.0.2

サービス提供装置署名：kkfrtyu.jhs68th1sh6s56s4hx1865ad

fg6856s4dg18swg1sh8srewat1g6h97d

【図4】

資金移動保証書

以下の金額を納入する

資金移動保証書番号：00001132

資金移動保証書要求番号：ABC0001

代行徴収金額：1000円

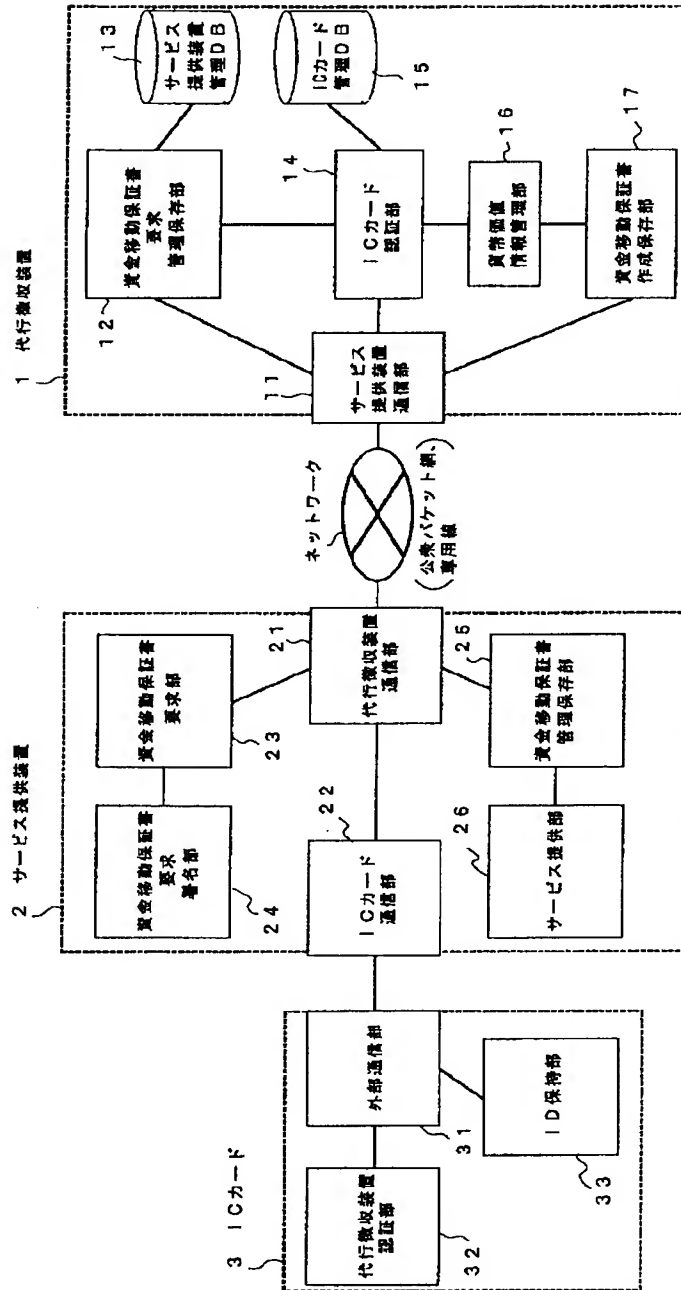
代行徴収金額納入先名：ABC株式会社

本書発行日時：1999/02/05/12:45:11

代行徴収装置署名：g32tlt6tlhgjk9kirl68it68auld56jhj1rti45id

1ghng3dduiui65f4kf1d54jd3jdeu

【図1】



【図2】

貨幣価値情報

ICカード内に格納したID番号	預かり金額(円)
00001	20000
00002	15000
00003	2350
⋮	⋮

【図6】

貨幣価値情報

ICカード内に格納したID番号あるいは代行徴収金額の納入先	預かり金額(円)
00001	20000
00002	15000
00003	2350
⋮	⋮
ABC株式会社	3500
DEF株式会社	11100
日本太郎	22350
⋮	⋮

【図8】

資金移動保証書

以下の金額を納入したことを保証する

資金移動保証書番号: 00001132

資金移動保証書要求番号: ABC10001

代行徴収金額: 1000円

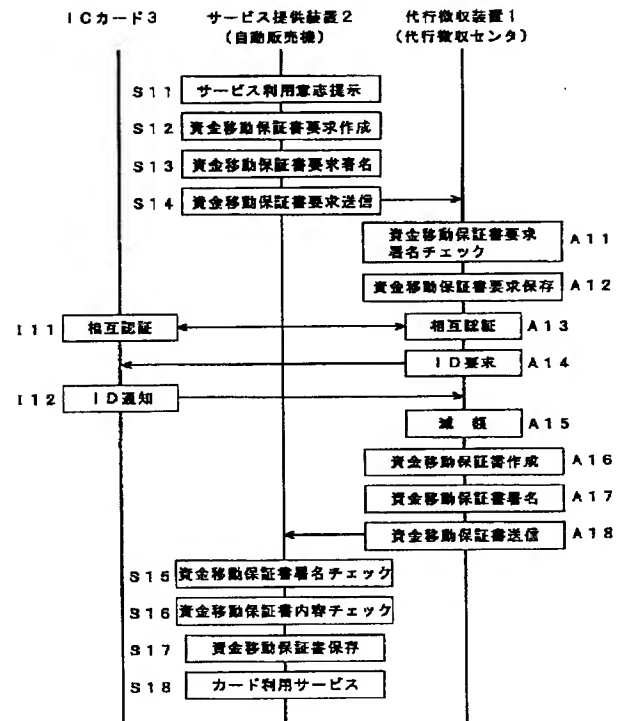
代行徴収金額納入先名: ABC株式会社

本書発行日時: 1999/02/05/12:45:11

代行徴収装置署名: I26n15o1u626nk154lk52jn1j5h1o1u1nk

I576hhv7f84v862626sq09gg1g

【図5】



【図7】

資金移動保証書要求

代行徴収を行うことを要求する

資金移動保証書要求番号: ABC1001

サービス提供装置名: ABC株式会社1番機

作成日時: 1999/02/05/12:45:09

代行徴収金額: 1000円

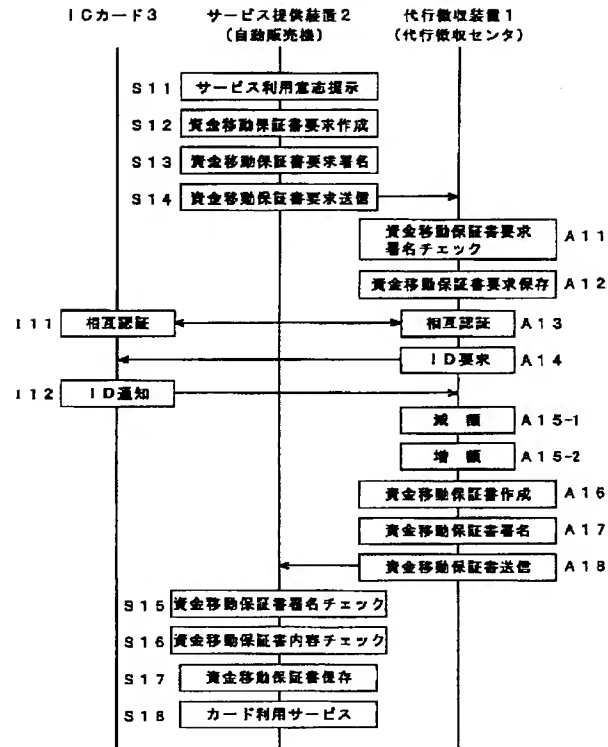
代行徴収金額納入先名: ABC株式会社

サービス提供装置IPアドレス: 129.0.0.2

サービス提供装置署名: kkfrtyujhs68th1sh6s56s4hx1865ad

fg6856s4dg18swg1sh8srewat1g6h97d

【図9】



フロントページの続き

(51) Int. Cl. ⁷	識別記号	F I	テームト* (参考)	
G 0 7 F	7/08	G 0 6 F	15/30	3 5 0 A
	7/10			3 6 0
		G 0 6 K	19/00	R
		G 0 7 F	7/08	Q

(72) 発明者	堀 正弘	F ターム (参考)	3E044 AA01 AA05 BA05 CA06 DD01
	東京都千代田区大手町二丁目3番1号 日		DE01
	本電信電話株式会社内		5B035 AA15 BB09 BC00
(72) 発明者	奥山 浩伸		5B049 AA05 BB17 BB46 CC39 DD04
	東京都千代田区大手町二丁目3番1号 日 40		EE23 GG02 GG04 GG07
	本電信電話株式会社内		5B055 BB10 CB09 EE02 EE12 EE27
			HA02 HB06 KK05 KK07
			5B058 CA40 KA33 KA40 YA02